IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In Re Application of:	
Brickell, et al.	Examiner: Truvan, Leynna Thanh
Application No.: 10/686,343	Art Unit: 2435
Filed: October 14, 2003	Confirmation No: 7197
For: METHOD FOR SECURELY DELEGATING TRUSTED PLATFORM MODULE OWNERSHIP	

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPEAL BRIEF UNDER 37 C.F.R. § 41.37(a)

This is an appeal to the Board of Patent Appeals and Interferences from the decision of the Examiner of Group 2435, dated December 23, 2008, in which Claims 1-2, 4-10, 12-18 and 20 of the above-identified application were finally rejected. The Office's date of receipt of Appellants' Notice of Appeal and Pre-Appeal Brief was April 23, 2009. This Appeal Brief is hereby submitted pursuant to 37 C.F.R. § 41.37(a), and in view of the Office's Notice of Panel Decision dated July 13, 2009.

I hereby certify that this correspondence is being deposited via EFS Web on the date below:

August 13, 2009
Date of Deposit

/Gigi Hoover/
Gigi Hoover

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The real party in interest and assignee of record is Intel Corporation, a corporation of Delaware having a principle place of business at 2200 Mission College Boulevard, Santa Clara, CA, 95052, United States of America.

II. RELATED APPEALS AND INTERFERENCES

To the best of Appellants' knowledge, there are no appeals or interferences related to the present appeal that will directly affect, be directly affected by, or have a bearing on the Board's decision in the instant appeal.

III. STATUS OF THE CLAIMS

Claims 1-2, 4-10, 12-18 and 20 are pending in the present application.

Claims 3, 11 and 19 have been canceled.

No Claims have been allowed.

Claims 1-2, 4-10, 12-18 and 20 have been finally rejected under 35 U.S.C. § 112, first paragraph, and 35 U.S.C. § 103(a) in the Final Office Action mailed December 23, 2008.

Claims 1-2, 4-10, 12-18 and 20 are the subject of this appeal. A copy of Claims 1-2, 4-10, 12-18 and 20 as they stand on appeal is set forth in Appendix A.

IV. STATUS OF AMENDMENTS

Subsequent to the Final Office Action mailed December 23, 2008 Appellant canceled no claims.

V. SUMMARY OF CLAIMED SUBJECT MATTER

This section of this Appeal Brief is set forth to comply with the requirements of 37 C.F.R. § 41.37(c)(1)(v) and is not intended to limit the scope of the claims in any way. Exemplary implementations of the features of claims 1-2, 4-10, 12-18 and 20 are described below.

Independent claim 1 is directed to a method of managing authorization tokens within a computer system. (*See* Appellants' specification, e.g., p. 11 lines 10-27 and Figure 3.) The method includes creating a master owner token indicating a management environment has full ownership of a trusted platform module within the computer system. (*See* Appellants' specification, e.g., p. 11 lines 12-17 and Figure 3, operations 300 and 302.) A delegate owner token is created for a delegated environment (*see* Appellants' specification, e.g., p. 11 lines 17-19 and Figure 3, operation 304), wherein the delegated environment is an environment to which the master owner token is not communicated. (*See* Appellants' specification, e.g., p. 5 line 6 – p. 6 line 2.) The delegate owner token is communicated to the delegated environment. (*See* Appellants' specification, e.g., p. 11 lines 19-20 and Figure 3, operation 306.) The delegated environment is allowed access to the trusted platform module when the delegated environment presents the delegate owner token to the trusted platform module. (*See* Appellants' specification, e.g., p. 11 lines 21-27 and Figure 3, operation 308.)

In claim 2, which depends from claim 1, the method further includes storing the master owner token in a secure storage within the computer system. (*See* Appellants' specification, e.g., p. 11 lines 16-17 and Figure 3, operation 302.)

In claim 4, which depends from claim 1, creating the delegate owner token includes the management environment sealing the delegate owner token to the delegated environment. (*See* Appellants' specification, e.g., p. 6 lines 4-13.)

In claim 5, which depends from claim 1, the method further includes the master owner token indicating the management environment can change at least one of the master owner token and the delegate owner token. (*See* Appellants' specification, e.g., p. 8 line 27 – p. 9 line 3.)

In claim 6, which depends from claim 1, the method further includes launching the management environment and then launching the delegated environment. (*See* Appellants' specification, e.g., p. 9 line 21 – p. 10 line 19.)

In claim 7, which depends from claim 1, the method further includes storing the delegate owner token in an access control list in the trusted platform module. (*See* Appellants' specification, e.g., p. 8 lines 17-26.)

In claim 8, which depends from claim 7, the method further includes removing, by the management environment, the delegate owner token from the access control list and adding a different delegate owner token to the access control list. (*See* Appellants' specification, e.g., p. 8 lines 17-26.)

Independent claim 9 is directed to a storage medium having a plurality of machine readable instructions, wherein when the instructions are executed by a processor (*see* Appellants' specification, e.g., p. 12 line 12 – p. 13 line 16), the instructions provide for a method of managing authorization tokens within a computer system. (*See* Appellants' specification, e.g., p. 11 lines 10-27 and Figure 3.) The method includes creating a master owner token indicating an administrative environment has full ownership of a trusted platform module within the computer system. (*See* Appellants' specification, e.g.,

p. 11 lines 12-17 and Figure 3, operations 300 and 302.) A delegate owner token is created for a delegated environment (*see* Appellants' specification, e.g., p. 11 lines 17-19 and Figure 3, operation 304), wherein the delegated environment is an environment to which the master owner token is not communicated. (*See* Appellants' specification, e.g., p. 5 line 6 – p. 6 line 2.) The delegate owner token is communicated to the delegated environment. (*See* Appellants' specification, e.g., p. 11 lines 19-20 and Figure 3, operation 306.) The delegated environment is allowed access to the trusted platform module when the delegated environment presents the delegate owner token to the trusted platform module. (*See* Appellants' specification, e.g., p. 11 lines 21-27 and Figure 3, operation 308.)

In claim 10, which depends from claim 9, the method further includes storing the master owner token in a secure storage within the computer system. (*See* Appellants' specification, e.g., p. 11 lines 16-17 and Figure 3, operation 302.)

In claim 12, which depends from claim 9, creating the delegate owner token includes the administrative environment sealing the delegate owner token to the delegated environment. (*See* Appellants' specification, e.g., p. 6 lines 4-13.)

In claim 13, which depends from claim 9, the method further includes the master owner token indicating the administrative environment can change at least one of the master owner token and the delegate owner token. (*See* Appellants' specification, e.g., p. 8 line 27 – p. 9 line 3.)

In claim 14, which depends from claim 9, the method further includes launching the administrative environment and then launching the delegated environment. (*See* Appellants' specification, e.g., p. 9 line 21 – p. 10 line 19.)

In claim 15, which depends from claim 9, the method further includes storing the delegate owner token in an access control list in the trusted platform module. (*See* Appellants' specification, e.g., p. 8 lines 17-26.)

In claim 16, which depends from claim 15, the method further includes removing, by the administrative environment, the delegate owner token from the access control list and adding a different delegate owner token to the access control list. (*See* Appellants' specification, e.g., p. 8 lines 17-26.)

Independent claim 17 is directed to a computer system. (*See* Appellants' specification, e.g., p. 10 line 20 – p. 11 line 9 and Figure 2.) The computer system includes a plurality of delegated environments (*see* Appellants' specification, e.g., p. 10 lines 24-25 and Figure 2, items 108 and 110) and a management environment. (*See* Appellants' specification, e.g., p. 10 line 21 and Figure 2, item 106.) The management environment creates a master owner token indicating the management environment has full ownership of a trusted platform module within the computer system (*see* Appellants' specification, e.g., p. 10 line 22 and Figure 2, item 120), to create a plurality of delegate owner tokens indicating partial ownership of the trusted platform module (*see* Appellants' specification, e.g., p. 10 lines 23-25 and Figure 2, item 124), and to communicate a selected one of the plurality of delegate owner tokens to a selected one of the plurality of delegated environments. (*See* Appellants' specification, e.g., p. 10 lines 25-26.) The selected one of the plurality of delegated environments is an environment to which the master owner token is not communicated. (*See* Appellants' specification, e.g., p. 5 line 6 – p. 6 line 2.) The trusted platform module stores delegate owner tokens created by the management environment and allows the selected one of the plurality of delegated environments access to the trusted platform module when the selected one of

the plurality of delegate owner tokens is presented to the trusted platform module by the selected one of the plurality of delegated environments. (*See* Appellants' specification, e.g., p. 11 lines 21-27.)

In claim 18, which depends from claim 17, the computer system further includes a secure storage to store the master owner token. (*See* Appellants' specification, e.g., p. 11 lines 16-17.)

In claim 20, which depends from claim 17, the trusted platform module includes an access control list for storing delegate owner tokens created by the management environment. (*See* Appellants' specification, e.g., p. 8 lines 17-26.)

VI. GROUNDS OF REJECTIONS TO BE REVIEWED ON APPEAL

Whether claims 1-2, 4-10, 12-18 and 20 are unpatentable under 35 U.S.C. § 112, first paragraph, and 35 U.S.C. § 103(a) as being unpatentable over Lambert in view of Challener.

VII. ARGUMENT

Claims 1-2, 4-10, 12-18 and 20 are pending in the above-referenced patent application, of which claims 1, 9 and 17 are independent claims. These independent claims are the main subject of this Appeal. These claims were finally rejected in the Final Office Action mailed December 23, 2008 (hereinafter "office action") under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement, and under 35 U.S.C. § 103(a) as being unpatentable over US 7,350,204 to Lambert et al. (hereinafter Lambert) in view of US 7,194,762 to Challener et al. (hereinafter Challener).

Claims 1-2, 4-10, 12-18 and 20 rejection under 35 U.S.C. §112, first paragraph

Claims 1-2, 4-10, 12-18 and 20 are rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement.

Independent claims 1 and 9, from which claims 2, 4-8, 10 and 12-16 depend, include the feature, "*the delegated environment is an environment* ***to which the master owner token is not communicated***." Independent claim 17, from which claims 18 and 20 depend, recites a similar feature. The office action states that the "*specification does not limit the claimed the delegated environment is an environment to which the master owner token is not communicated.*" (*See* office action, p. 6, second paragraph.)

On the contrary, the specification does indeed support the claimed feature, "*wherein the delegated environment is an environment to which the master owner token is not communicated.*" Citing § 2163 of the M.P.E.P.,

> "To comply with the written description requirement of 35 U.S.C. 112, para. 1 each claim limitation must be **expressly, implicitly**, or inherently supported in the originally filed disclosure. When an explicit limitation in a claim "is not present in the written description whose benefit is sought it must be shown that a person of ordinary skill would have understood, at the time the patent application was filed, that the description requires that limitation." *Hyatt v. Boone*, 146 F.3d 1348, 1353, 47 USPQ2d 1128, 1131 (Fed. Cir. 1998)." (§ 2163 of the M.P.E.P. Emphasis added.)

The Appellants respectfully assert that the feature, "*wherein the delegated environment is an environment to which the master owner token is not communicated,*" is present in the originally filed written description both expressly and implicitly. The specification states:

> "In one embodiment, there is correspondence between environments and tokens. **An environment controls a token (master or delegate) if that environment is the only environment that is given access to that token**." In an example, "an environment can control a token by having the user input the token into the environment." (*See* Appellants' specification, p. 6, lines 23-29.)

It follows that, in the embodiment disclosed, if a master token were communicated to a delegated environment, either the master token would no longer be a master token, as defined above, or the delegated environment would no longer be a delegated environment, as is also defined above. That is, the master owner token is not communicated to the delegated environment. Thus, there is explicit support for the claimed feature, "*wherein the delegated environment is an environment to which the master owner token is not communicated.*"

Furthermore, in the embodiment disclosed, an environment can control a token by having the user input the token into the environment, as recited above. One of ordinary skill in the art at the time would have understood that user input of a token to an environment is a form of communication of the token to the environment. The user input and, hence, the communication is limited by the definitions above for types of tokens and corresponding environments, as disclosed in the specification. For example, if a master token were input by a user to a delegated environment, either the master token would no longer be a master token, as defined above, or the delegated environment would no longer be a delegated environment, as is also defined above. That is, the master owner token is not communicated to the delegated environment. Accordingly, there is implicit support for the claimed feature, "*wherein the delegated environment is an environment to which the master owner token is not communicated.*" Thus, claims 1-2, 4-10, 12-18 and 20 comply with the written description requirement.

Claims 1-2, 4-10, 12-18, and 20 rejection under 35 U.S.C. §103(a)

Claims 1-2, 4-10, 12-18, and 20 are rejected under 35 U.S.C. §103(a) as being unpatentable over Lambert in view of Challener.

Independent claims 1 and 9, from which claims 2, 4-8, 10 and 12-16 depend, include the feature, "*the delegated environment is an environment* ***to which the master owner token is not communicated***." Independent claim 17, from which claims 18 and 20 depend, recites a similar feature.

The office action relies solely on Lambert to disclose the portion of the claims that state, i.e. to anticipate the feature, "*wherein the delegated environment is an environment to which the master owner token is not communicated.*" However, Lambert fails to anticipate this feature. Citing § 2131.01 of the M.P.E.P.,

> ""A claim is anticipated only if each and every element as set forth in the claim is found, **either expressly or inherently described**, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)." (§ 2163 of the M.P.E.P. Emphasis added.)

Thus, if a single reference is used reject an element of a claim, that single reference must disclose the element either expressly or inherently. Lambert does neither. The office action points out, Lambert "*does not suggest the parent token is communicated to the delegated environment since the focus is the restricted token that is associated to a process/software.*" (*See* office action, p. 8, first paragraph.) However, **the lack of suggestion referred to by the office action is certainly not an explicit disclosure** that the parent token of Lambert is not communicated to the delegated environment, because it is not stated explicitly that this is the case. Furthermore, **the lack of suggestion in Lambert is also not an inherent disclosure** that the parent token of Lambert is not communicated to the delegated environment, because none of the technical features disclosed by Lambert would restrict the parent token of Lambert from being communicated to the delegated environment. Accordingly Lambert fails to disclose

"*wherein the delegated environment is an environment to which the master owner token is not communicated*," as taught and claimed by the Appellants.

Challener is relied on merely to disclose "*a method and system for improved security password-based access to computer networks*," including the use of "*a Trusted Platform Module*." (*See* office action, p. 8, second paragraph.) As such, Challener fails to cure the above-noted deficiencies of Lambert. Thus, **neither Lambert nor Challener, alone or in combination, discloses "the delegated environment is an environment to which the master owner token is not communicated,"** as taught and claimed by the Appellants.

VIII. CONCLUSION

For at least the reasons stated above, claims 1-2, 4-10, 12-18 and 20 are patentable. Appellant respectfully requests that the Board reverse the rejections of claims 1-2, 4-10, 12-18 and 20 under U.S.C. § 102(e)/103(a) and direct the Examiner to enter a Notice of Allowance for claims 1-2, 4-10, 12-18 and 20.

Fee For Filing A Brief In Support Of Appeal

Enclosed is a check in the amount of $540.00 to cover the fee for filing a brief in support of an appeal as required under 37 C.F.R. 1.17(c) and 40.20(b)(2). (If a check is not enclosed, you are hereby authorized to charge the deposit account below).

Deposit Account Authorization

Authorization is herby given to charge our Deposit Account No. 02-2666 for any charges that may be due. Furthermore, if an extension is required, then Appellant hereby requests such extension.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: August 13, 2009

/Justin K. Brask/

Justin K. Brask
Reg. No. 61,080

Blakely, Sokoloff, Taylor & Zafman LLP
1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
Telephone: (503) 439-8778
Facsimile: (503) 439-6073

APPENDIX A : CLAIMS

Listing of Claims:

1. (Previously presented) A method of managing authorization tokens within a computer system comprising:

creating a master owner token indicating a management environment has full ownership of a trusted platform module within the computer system;

creating a delegate owner token for a delegated environment, wherein the delegated environment is an environment to which the master owner token is not communicated;

communicating the delegate owner token to the delegated environment; and

allowing the delegated environment access to the trusted platform module when the delegated environment presents the delegate owner token to the trusted platform module.

2. (Original) The method of claim 1, further comprising storing the master owner token in a secure storage within the computer system.

3. (Canceled)

4. (Previously presented) The method of claim 1, wherein creating the delegate owner token comprises the management environment sealing the delegate owner token to the delegated environment.

5. (Previously presented) The method of claim 1, further comprising the master owner token indicating the management environment can change at least one of the master owner token and the delegate owner token.

6. (Previously presented) The method of claim 1, further comprising launching the management environment and then launching the delegated environment.

7. (Previously presented) The method of claim 1, further comprising storing the delegate owner token in an access control list in the trusted platform module.

8. (Previously presented) The method of claim 7, further comprising removing, by the management environment, the delegate owner token from the access control list and adding a different delegate owner token to the access control list.

9. (Previously presented) An article comprising:

a storage medium having a plurality of machine readable instructions, wherein when the instructions are executed by a processor, the instructions provide for managing authorization tokens within a computer system by

creating a master owner token indicating an administrative environment has full ownership of a trusted platform module within the computer system;

creating a delegate owner token for a delegated environment, wherein the delegated environment is an environment to which the master owner token is not communicated;

communicating the delegate owner token to the delegated environment; and

allowing the delegated environment access to the trusted platform module when the delegated environment presents the delegate owner token to the trusted platform module.

10. (Original) The article of claim 9, further comprising instructions for storing the master owner token in a secure storage within the computer system.

11. (Canceled)

12. (Previously presented) The article of claim 9, wherein creating the delegate owner token comprises the administrative environment sealing the delegate owner token to the delegated environment.

13. (Previously presented) The article of claim 9, further comprising the master owner token indicating the administrative environment can change at least one of the master owner token and the delegate owner token.

14. (Previously presented) The article of claim 9, further comprising instructions for launching the administrative environment and then launching the delegated environment.

15. (Previously presented) The article of claim 9, further comprising instructions for storing the delegate owner token in an access control list in the trusted platform module.

16. (Previously presented) The article of claim 15, further comprising instructions for removing, by the administrative environment, the delegate owner token from the access control list and adding a different delegate owner token to the access control list.

17. (Previously presented) A computer system comprising:

a plurality of delegated environments;

a management environment to create a master owner token indicating the management environment has full ownership of a trusted platform module within the computer system, to create a plurality of delegate owner tokens indicating partial ownership of the trusted platform module, and to communicate a selected one of the plurality of delegate owner tokens to a selected one of the plurality of delegated environments, wherein the selected one of the plurality of delegated environments is an environment to which the master owner token is not communicated;

wherein the trusted platform module stores delegate owner tokens created by the management environment and allows the selected one of the plurality of delegated environments access to the trusted platform module when the selected one of the plurality of delegate owner tokens is presented to the trusted platform module by the selected one of the plurality of delegated environments.

18. (Original) The computer system of claim 17, further comprising a secure storage to store the master owner token.

19. (Canceled)

20. (Previously presented) The computer system of claim 17, wherein the trusted platform module comprises an access control list for storing delegate owner tokens created by the management environment.

APPENDIX B: EVIDENCE

NONE

APPENDIX C: RELATED PROCEEDINGS

NONE